WHAT IS CLAIMED IS:

1. A method of network computing:

using a server with a virus monitor to identify a client computer that is infected with a virus or susceptible to a virus; and

isolating the virus-infected client computers and virus-susceptible client computers from the server and from a computing network connected to the server.

2. The method of claim 1 wherein the using step further comprises:

scanning the client computer with a virus monitor of at least one of the server and the client computer.

3. The method of claim 1 wherein the isolating step further comprises:

tracking a client identifier of the virus-infected and virus-susceptible client computers; and

preventing a client-server connection and network communications between the virus-infected client computers and virus-susceptible client computer and the computing network.

4. The method of claim 1 wherein the using and isolating steps further comprise:

detecting client computers that do not maintain an enabled virus protector; and

terminating a client-server connection for client computers that have a disabled virus protector.

5. The method of claim 1 wherein the using and isolating steps further comprise:

detecting client computers that are not enabled for virus protection during an attempted client server connection; and

preventing a client-server connection for those non-enabled client computers.

6. A method of virus-controlled network access comprising:

using a server of a network with a virus monitor to identify client computers that fail to produce an approved virus scan report; and

isolating client computers without an approved virus scan report from authorized communication with the server.

7. A method of maintaining a virus-controlled network computing system comprising:

booting a client computer to establish a client-server connection with a server and to scan the client computer for a virus;

reporting the results of the virus scan from the client computer to the server;

selectively permitting the client computer authorized access to the server through the client-server connection when the virus scan report detects no viruses and denying the client computer access to the server when a virus is detected or no valid virus report is provided by the client computer.

8. The method of claim 7 and further comprising:

establishing the client-server connection based on the client computer maintaining a virus protector of the client computer in an enabled mode.

9. The method of claim 7 wherein the terminating step further comprises:

querying the client periodically to determine if the virus protector of the client computer remains enabled.

10. The method of claim 7 and further comprising:

terminating the client-server connection if the virus definitions of the virus protector of the client computer have not been updated within a specified date criteria of the server.

11. A method of preventing network virus migration within a network comprising:

monitoring a virus susceptibility of each client computer of the network; and

tracking virus susceptible client computers and preventing a client-server connection between each virus-susceptible client computer and the server.

12. The method of claim 11 wherein the monitoring step further comprises:

determining virus susceptibility based on whether a virus protector of the client computer is enabled.

13. The method of claim 11 wherein the monitoring step further comprises:

determining virus susceptibility based on whether the client computer presented the server with a valid virus scan report.

14. The method of claim 11 wherein the tracking and preventing step further comprise:

terminating the client-server connection for at least one of a virus susceptible client computer and a virus-infected client computer.

15. The method of claim 14 wherein the tracking and preventing step further comprise:

identifying an address of each virus-susceptible and virus-infected client computer to selectively prevent further client-server connections with those client computers by establishing a quarantine of the identified client computers.

16. A virus exclusion network system comprising:

a client computer including a virus protector;

a network server including a virus monitor configured for preventing an authorized network connection between the client computer and the server when

the client computer fails to produce at least one of a report of an up-to-date virus scan of the client computer and a confirmation of enablement of the virus protector of the client computer.

17. The system of claim 16 wherein the client computer further comprises:

a virus protector for scanning the client computer for viruses.

18. The system of claim 16 wherein the virus monitor of the server further comprises:

a virus protector for scanning the client computer and files written by the client computer.

19. A server comprising:

a controller;

a virus monitor including:

a virus protector with a scanning function;

a virus definition source; and

a quarantine monitor configured for preventing a client-server connection for client computers that are virus-infected or virus-susceptible and configured for tracking an identity of those client computers.

20. A client computer comprising:

a controller;

a virus protector configured for detecting and eradicating viruses on the client computer, for maintaining real-time virus protection, and for producing a report to a server to confirm that the client computer is virus-free and thereby eligible to connect to the server with authorized access privileges.

21. A computing network virus monitor comprising:

a virus protector;

a quarantine monitor configured for preventing network communications originating from a client computer that is virus-infected or virus-susceptible and configured for tracking an identity of those client computers.

22. A virus quarantine monitor of a server comprising:

a client computer identifier;

a virus identifier; and

a blocking mechanism configured for signaling the server to prevent client-server connections with client computers identified as being virus susceptible or virus-infected.

23. A computer-readable medium having computer-executable instructions for performing a method of network virus exclusion, the method comprising:

identifying client computers that are at least one of virus-susceptible and virus-infected; and

isolating virus-susceptible client computers and virus-infected client computers from authorized communication with a server of the network.

24. A computer-readable medium having computer-executable instructions for performing a method of preventing network virus migration within a network, the method comprising:

monitoring a virus susceptibility of each client computer of the network; and

tracking virus susceptible client computers and preventing a client-server connection between each virus-susceptible client computer and the server.

25. A computer-readable medium having computer-executable instructions for performing a method of network computing, the method comprising:

using a server with a virus monitor to identify a client computer that is infected with a virus or susceptible to a virus; and

isolating the virus-infected client computers and virus-susceptible client computers from the server and from a computing network connected to the server.

26. A computer-readable medium having computer-executable instructions for performing a method of monitoring network connections, the method comprising:

preventing an authorized network connection between a client computer and a server when the client computer fails to produce at least one of a report of an up-to-date virus scan of the client computer and a confirmation of enablement of the virus protector of the client computer.

27. A computer-readable medium having computer-executable instructions for performing a method of quarantining client computers, the method comprising:

preventing a client-server connection for client computers that are virus-infected or virus- susceptible; and

tracking an identity of the virus-infected and virus-susceptible client computers.